Virginia Department of Social Services

Information Security Policy

Issued: May 2007

PREFACE

Subject

VDSS Information Security Policy

Effective Date

March 1, 2007

Compliance Date

July 1, 2007

Publication Revision History

Original	July 15, 1992
Revision 1	April 3, 2001
Revision 2	November 18, 2003
Revision 3	MMDD, 2006

Authority

The policies described in this document are based on requirements found in the following codes, policies, regulations, laws, standards and guidelines:

Code of Virginia § 2.2-603(F) (Authority of Agency Directors)

Code of Virginia, §2.2-2827 (Restrictions on state employee access to information infrastructure)

Code of Virginia §2.2-3803 (Administration of systems including personnel information; Internet privacy policy)

Code of Virginia, §2.2-3800 (Government Data Collection and Dissemination Practices Act)

Code of Virginia, Chapter 52

TANIF Manual 103.1 (1/20/97), Purpose of Safeguarding of Information and Scope of Regulations

VDSS/DCSE Manual, Chapter 2 (11/1/96), Confidentiality/Information Release

USDA/FNS 7 CFR .72.1(c), 272.1(d), Disclosure of Information

HHS 45 CFR 303.21 and 45 CFR 303.105

IRS Revenue Procedure Section 6103 (L)(7)(b), Disclosure of Information to Federal, State, and Local Agencies

Public Law 100-235, Computer Security Act of 1987

Virginia Social Service Laws 63.2 (2002)

Virginia State Library and Archives, Records Retention and Disposition Schedules (RM-2) (7/94)

ITRM Policy SEC500-02

ITRM Standard SEC501-01

Scope

This policy applies to:

All *Individuals* (VDSS employees, employees of local social service agencies (LSSA), contractors, vendors, volunteers, work experience personnel and other persons and organizations) who have a need to use DSS related information or information processing systems;

All information and information processing systems associated with the Department of Social Services; and

All information and information processing systems associated with other organizations which the Department of Social Services uses, including but not limited to SSA, TAX, IRS, DMV, and VEC.

In accordance with the *Code of Virginia* § 2.2-603, § 2.2-2009, and § 2.2-2010 the VDSS is responsible for complying with Commonwealth ITRM policies and standards and considering Commonwealth ITRM guidelines issued by the CIO. In addition: *"The director of every department in the executive branch of state government shall report to the Chief Information Officer as described in, all known incidents that threaten the security of the Commonwealth's databases and data communications resulting in exposure of data protected by federal or state laws, or other incidents compromising the security of the Commonwealth's information technology systems with the potential to cause major disruption to normal agency activities. Such reports shall be made to the Chief Information Officer within 24 hours from when the department discovered or should have discovered their occurrence."*

Regulatory References

1. Privacy Act of 1974.
2. Internal Revenue Codes 6103(d), 6103(b)(4), and 6103(p).
3. Social Security Act paragraphs 464 and 1137.
4. Children's Online Privacy Protection Act.
5. Family Educational Rights and Privacy Act.
6. Executive Order of Critical Infrastructure Protection.
7. Federal Child Pornography Statute: 18 U.S.C. & 2252
8. FDA CFR 21, Part 11.
9. Executive Order 13231
10. USA Patriot Act of 2001.
11. Bank Secrecy Act.
12. Virginia Computer Crime Act, *Code of Virginia*, §18.2-152.3.,4., 5., and 6.
13. Library of Virginia Records Management Program, *Code of Virginia*, Title 42.1, Chapter 7, sec 42.1-85.
14. California Database Breach Notification Act.
15. Federal Information Security Management Act (FISMA).
16. Notification of Risk to Personal Data.
17. Office of Management and Budget (OMB) Circular A-130.
18. Tax Information Security Guidelines For Federal, State and Local Agencies Publication 1075

Definitions See Glossary

TABLE OF CONTENTS

1. INFORMATION SECURITY POLICY STATEMENT

1.1 Background

The Virginia Department of Social Services (VDSS) relies heavily on the application of information technology for the effective delivery of benefit and services programs. Rapid and continuing technical advances have increased the dependence of state and local agencies on information systems. The value of VDSS information, software, hardware, telecommunications, and facilities is an important resource and must be protected.

1.2 Guiding Principles

The following principles guide the development and implementation of VDSS information security management and practices.

a. Information is:

   1. A critical asset that shall be protected.

   2. Restricted to authorized personnel for official use.

b. Information security must be:

   1. A cornerstone of maintaining public trust.

   2. Managed to address both business and technology requirements.

   3. Risk-based and cost-effective.

   4. Aligned with VDSS priorities, prudent industry practices, and government requirements.

   5. Directed by policy but implemented by business owners.

   6. Everybody's responsibility.

1.3 Purpose

The purpose of the DSS Information Security Policy is to:

a. Promote information security awareness to individuals using VDSS systems and information;

b. Make each of us aware of our duty to protect VDSS' information and information processing systems;

c. Ensure the confidentiality, availability, and integrity of data;

d. Reduce the risk of data loss by accidental or intentional modification, disclosure, or destruction; and

e. Preserve VDSS's rights and remedies in the event of such a loss.

1.4 Statement of Policy

The Commissioner is responsible for the security of the Department's data including case records and documents containing client or confidential information; and for taking appropriate steps to secure Department IT systems and data through the Department's Information Security Program. This policy and related standards provides the minimum security requirements that apply to all divisions, offices and local social service agencies. Exceptions to this policy must be clearly documented, reviewed and approved by the VDSS Information Security Officer (ISO).

The function of the policy is to protect the VDSS' information assets from creditable threats, whether internal or external, deliberate or accidental. It is the policy of the VDSS to use all reasonable security control measures to:

a. Ensure confidentiality of department information by protecting department information and information systems against unauthorized access or disclosure;

c. Maintain the integrity of department data;

d. Meet requirements for availability of information and information systems, allowing the department the ability to provide services and benefits to its customers;

e. Meet federal, state and other regulatory and legislative requirements; and

f. Ensure business continuity in the event of a catastrophic event.

Violations of this policy must be reported to the appropriate division/office/agency director and the VDSS Information Security Officer. Depending on the severity, an employee who violates these policies may receive a Standards of Conduct Offense. Violations of state and local laws will be reported to the appropriate law enforcement authorities. Prosecuting action may be undertaken if a person knowingly and intentionally violates any local, state or federal laws or use any VDSS related information, information processing systems or equipment for fraudulent, extortive or destructive purposes.

In the case of lost or missing computer equipment or software, notification must also be made immediately to the Information Security Officer.

2. ROLES AND RESPONSIBILITIES

2.1 Policy

Each division, office, region, district and local social service agency must have an effective security administration function in place. For an information security program to be effective, someone in each division, office, region, district and local social service agency should be assigned the responsibility for administering the security program in their unit. The individual selected should be cognizant of data processing and information security fundamentals and possess sufficient abilities to understand, implement and enforce information security policies and procedures.

Each division, office, district, region and local social service agency must designate a security officer and at least one backup security officer whose responsibility is to ensure compliance with the VDSS Information Security Policies and Standards.

2.2 Commissioner

The Commissioner is responsible for the security of the Department's Information Technology (IT) systems and data including case records and documents containing client or confidential information. The Commissioner, through the Information Security Unit, is responsible for assuring that Information Security Policies are developed and distributed to all VDSS and local social service agency staff, contractors, vendors and other persons and organizations who have a need to use VDSS related information and information processing systems. The Commissioner is responsible for final interpretation of this policy.

The Commissioner's responsibilities include the following:

a. Designate an Information Security Officer and Backup Information Security Officer for the Department and ensuring the shortest practicable reporting lines to the Commissioner.

b. Maintain an IT security program that is sufficient to protect the Department's IT systems and the program is documented and effectively communicated.

c. Approve a business impact analysis (BIA), a risk assessment (RA), and a Continuity of Operations Plan (COOP) to include an IT disaster recovery plan.

d. Facilitate the communication process between data processing staff and those in other areas of the Department.

e. Establish a program of IT security safeguards.

f. Establish and provide for an IT security awareness and training program

g. Provide the resources to enable employees to carry out their responsibilities for securing IT systems and data.

h. Maintain compliance with IT Security Audit Standards.

i. Accept residual risk as described in section 2.5 of the IT Security Audit Standard (COV ITRM Standard SEC5007-00).

2.3 Division/Office/District/Regional/Local Agency Management

Managers at all levels are responsible for the security of the Department's IT systems and data including case records and documents containing client or confidential information under their jurisdiction. They shall take all reasonable actions to provide adequate security and to escalate problems, requirements, and matters related to IT security to the highest level necessary for resolution.

Division, office, district, regional and local social service agency directors are responsible for:

a. Appointing security officers and backup security officers;

b. Implementing, and enforcing procedures within their units which ensure compliance with VDSS Information Security Policies and Standards;

c. Ensuring violations or suspected violations of VDSS Information Security Policy are reported to the DSS Information Security Officer; and

d. Ensuring that all users of VDSS information and information systems are made aware of VDSS Information Security Policies and Standards and receive continuing security training.

2.4 All Personnel

All personnel including VDSS employees, local social service agency employees, contractors, volunteers, business partners, and any other users of VDSS information systems and resources are responsible for the following:

a. Reading and complying with the Department of Social Services' Information Security Policies.

b. Reading and signing the Information Security Policy Acknowledgement (ISPA).

c. Doing everything reasonable within their power to ensure that the Department's Information Security Policy is implemented, maintained, and enforced.

d. Reporting breaches of information security, actual or suspected, to appropriate management and the VDSS ISO.

e. Taking reasonable and prudent steps to protect the security of IT systems and data to which they have access.

2.5 Information Security Officer (ISO)

The Information Security Officer is responsible for developing and managing the Department's Information Security Program. The ISO duties are as follows:

a. Develop and manage an IT security program that meets or exceeds the requirements of COV IT security policies and standards in a manner commensurate with risk.

b. Develop and maintain an IT security awareness and training program for Department and local social service agency staff, including contractors, volunteers and service providers.

d. Coordinate and provide IT security information to the VITA CISO as required;

e. Implement and maintain the appropriate balance of protective, detective and corrective controls for VDSS IT systems commensurate with data sensitivity, risk and system criticality.

f. Mitigate and report all IT security incidents in accordance with §2.2-603 of the *Code of Virginia* and VITA requirements and take appropriate actions to prevent recurrence.

g. Maintains liaison with the Commonwealth's CISO.

2.6 VDSS Information Security Unit

The VDSS Information Security Unit is responsible for providing technical information, security assistance, and fostering and overseeing the Department's information security program. Specific responsibilities include but are not limited to:

a. Providing technical assistance to divisions, offices, districts, regions and local social service agencies in developing, implementing and administering their security programs and procedures;

b. Developing, maintaining and disseminating Information Security Polices, Standards and Guidelines, ensuring their uniform interpretation and implementation throughout state VDSS offices and local social service agencies;

c. Participating in VDSS System Development activities to ensure an appropriate level of security, confidentiality and availability is provided to VDSS systems.

d. Performing business impact analysis and risk assessment studies for VDSS' information technology systems;

e. Developing, maintaining and disseminating a disaster recovery plan for the Division of Information Systems and performing an annual disaster recovery test;

f. Training workers on the security features of VDSS' systems; and

g. Reviewing security incident reports and coordinating corrective action to prevent a similar occurrence. Investigate alleged security breaches.

2.7 Security Officers

Division, office, district, regional and local social service agency security officers serve as the point of contact for all security related matters in their divisions, offices and agencies. Security officer are empowered by their director to make decisions regarding the protection of VDSS information, resources and user access privileges to ensure VDSS information and resources are protected from misuse or abuse. Security officers are responsible for:

a. Administering user access privileges to DSS information systems and resources.

b. Verifying the access privileges of active employees.

c. Communicating security-related events to the VDSS ISO.

d. Attending annual security training sponsored by VDSS.

e. Providing security training to their local staff annually.

2.8 System Owner (VDSS Division Directors and their designees)

The System Owner is the Department manager responsible for making system-related development and maintenance decisions and establishing priorities. With respect to IT security, the System Owner's responsibilities include the following:

a. Require that all IT system users complete required IT security awareness and training activities prior to, or as soon as practicable after, receiving access to the system, and no less than annually, thereafter.

b. Manage system risk and developing any additional IT security policies and procedures required to protect the system in a manner commensurate with risk.

c. Maintain compliance with VDSS IT security policies and standards in all IT system activities.

d. Maintain compliance with requirements specified by Data Owners for the handling of data processed by the system.

e. Designate a System Administrator for the system.

2.9 Data Owner (VDSS Division Directors and their designees)

The Data Owner is the Department manager responsible for the policy and practice decisions regarding data including case records and documents containing client or confidential information and is responsible for the following:

a. Evaluate and classify sensitivity of the data.

b. Define protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs.

c. Communicate data protection requirements to the System Owner.

d. Define requirements for access to the data.

2.10 **Data Owner** (Local Social Service Agency Directors)

Directors of Local Social Service Agency that enter data supplied by VDSS into local systems are responsible for the security of the local Information Technology (IT) systems and data contained therein. The local director is responsible for assuring that Information Security Policies are developed and distributed to all local social service agency staff, contractors, vendors and other persons and organizations that use local systems that process or store VDSS provided information. The local director is responsible for final interpretation of local IT Security Policy.

The local director's data ownership responsibilities include:

a. Establishing and maintaining an IT security program for local systems that process or store VDSS provided information (i.e. Harmony, EZ-filer) that includes:

- Developing and distributing Information Security Policies and Standards to all individuals who use local systems that process or store VDSS provided information.

- Establishing and providing IT security awareness and training relevant to local systems.

b. Providing for both physical and logical separation of duties by ensuring no one person has sole control of sensitive processes.

2.11 Data Custodian

Data Custodians are individuals or organizations in physical or logical possession of data for Data Owners. Data Custodians are responsible for the following:

a. Protect the data in their possession from unauthorized access, alteration, destruction, or usage.

b. Establish, monitoring, and operating IT systems in a manner consistent with VDSS IT security policies and standards.

c. Provide Data Owners with reports, when necessary and applicable.

2.12 System Administrators (VDSS Division of Information Systems)

The Systems Administrator is an analyst, engineer or consultant who implements, manages and/or operates a system or systems at the direction of the System Owner and/or Data Custodian. The Systems Administrator assists department management in the day-to-day administration of the department's IT systems and implements security controls and other requirements of the department's IT security program on the IT systems for which the Systems Administrator have been assigned responsibility. Systems administrators are appointed by the Department's Chief Information Officer (CIO).

3. Laws and Penalties

3.1 Laws

Privacy Act of 1974. Provides that unauthorized access to or disclosure of personal information in any manner to any person or agency not entitled to receive it is a misdemeanor. Violators are subject to a fine of not more than $5,000.

Internal Revenue Code (IRC 7213 & 7431). Provides that unauthorized disclosure of any information provided by the IRS is a felony punishable by a fine not to exceed $5,000 or imprisonment for not more than 5 years or both. Taxpayers may also bring civil action for damages sustained by the plaintiff as a result of such unauthorized disclosure.

Fair Credit Reporting Act. Under this law, obtaining information under false pretenses or unauthorized disclosure of information is punishable by a fine of up to $5,000 or one year's imprisonment or both. Consumers may also bring civil suit for damages they sustain, and the court may also award a civil penalty of up to $1,000 for knowing and willful violations.

Freedom of Information Act. This act opens agency records to the public but requires the agency to ensure that policies and procedures are in place to review requests for information and deny release of protected and sensitive information. It provides for a civil penalty of up to $1,000 for knowing and willful violations.

3.2 Penalties

Employees who violate the Information Security Policy may be subject to a Standards of Conduct. Violations by others may result in actions which Executive Management deems appropriate. VDSS cooperates with law enforcement agencies in the investigation and prosecution of any violations of these laws.

4. IT SECURITY PROGRAM

The VDSS ISO is charged with developing and administering the VDSS IT security program in a manner that meets Department business needs, protects IT systems and data in a manner commensurate with data sensitivity and risk, and, at a minimum, meets the requirements of COV IT policies and standards. VDSS requirements for the implementation of the following IT Security Program requirements can be found in the VDSS Information Security Standards. While the majority of these security program components are VDSS' responsibility, those infrastructure related components are the responsibility of VITA/NG.

4.1 Risk Management

This policy and related standards are based on protecting VDSS systems and data based on sensitivity and risk, including system availability needs. Accordingly, Risk Management is a central component of the Department's IT security program and allows the Department to determine how these factors apply to its IT systems.

The first step in Risk Management is a Business Impact Analysis (BIA). BIA is a process of analyzing the Department's business functions, to identify those that are essential or those that contain sensitive data, and assessing the resources that support them. For the purposes of IT security, the BIA identifies those business functions that are essential or involve sensitive data and that are dependent on IT. This analysis is necessary in order to determine the appropriate level of protection for IT systems and the data they process.

After completing the BIA, the Department will document and characterize the types of data it handles, and classify the sensitivity of IT systems and data for use in the Risk Assessment (RA) process. Sensitivity must consider the elements of availability, confidentiality and integrity.

The Department then defines, inventories, and determines ownership of all IT systems classified as sensitive so that IT security roles can be appropriately assigned.

A periodic, formal RA is required for all IT systems classified as sensitive. While a formal RA is not required for IT systems that are not sensitive, an informal risk analysis should be conducted on those IT systems and the data they handle, and to apply appropriate additional IT security controls as required. The RA process assesses the threats to IT systems and data, probabilities of occurrence and the appropriate IT security controls necessary to reduce these risks to an acceptable level.

After appropriate mitigating IT security controls have been applied relative to sensitivity and risk, based on RA results, sensitive IT systems require periodic, independent IT Security Audits. These audits are necessary to determine whether the overall protection of IT systems and the data they handle is adequate and effective. The requirements for IT Security Audits are discussed in more detail in Section 5 of this document, and in the *IT Security Audit Standard* (COV ITRM Standard SEC502-00).

IT Security Audits may identify additional mitigating controls for sensitive IT systems in order to provide adequate and effective protection of the systems and the data they handle. After applying these controls, the final step in the Risk Management process is formal acceptance by the Commissioner or designee of any residual risk to Department's operations from sensitive IT systems.

4.2 IT Contingency Planning

IT Contingency Planning defines processes and procedures that plan for and execute recovery and restoration of IT systems and data that support essential business functions if an event occurs that renders the IT systems and data unavailable. IT Contingency Planning includes Continuity of Operations Planning, Disaster Recovery Planning, and IT System Backup and Restoration.

A key element of IT contingency planning is Continuity of Operations Planning, which provides a business continuation strategy for essential VDSS business functions as identified in the BIA. These processes may or may not be dependent on IT resources. The Virginia Department of Emergency Management (VDEM) provides the COV guidance on Continuity of Operations Plans (COOP).

Disaster Recovery Planning supports COOP by defining specific policies, processes, standards, and procedures for restoring IT systems and data that support essential business functions, on a schedule that supports VDSS' mission requirements.

Based on related elements in the IT contingency planning process, IT System Backup and Restoration defines plans and restoration schedules that meet VDSS' mission requirements for the backup and restoration of data.

4.3 IT Systems Security

The purpose of IT systems security is to define the steps necessary to provide adequate and effective protection for VDSS IT systems in the areas of IT System Hardening, IT Systems Interoperability Security, Malicious Code Protection, and IT Systems Development Life Cycle Security. The Department's IT systems may require further security controls for adequate protection based on the identification of sensitivity and risk to these systems, including system availability needs, identified through Risk Management policies, processes, and procedures.

4.4 Logical Access Control

Logical Access Control requirements define the steps necessary to protect the confidentiality, integrity, and availability of VDSS systems and data against compromise. Logical Access Control requirements identify the measures needed to verify that all IT system users are who they say they are and that they are permitted to use the systems and data they are attempting to access. Logical Access Control defines requirements in the areas of Account Management, Password Management, and Remote Access.

4.5 Data Protection

Data Protection provides security safeguards for the processing and storing of data. This component of the VDSS Security Program outlines the methods that can use to safeguard the data in a manner commensurate with the sensitivity and risk of the data stored. Data Protection includes requirements in the areas of Media Protection and Encryption.

4.6 Facilities Security

Facilities Security safeguards require planning and application of facilities security practices to provide a first line of defense for IT systems against damage, theft, unauthorized disclosure of data, loss of control over system integrity, and interruption to computer services.

4.7 Personnel Security

Personnel Security controls reduce risk to VDSS systems and data by specifying Access Determination and Control requirements that restrict access to these systems and data to those individuals who require such access as part of their job duties. Personnel Security also includes Security Awareness and Training requirements to provide all IT system users with appropriate understanding regarding VDSS security policies and Acceptable Use requirements for the Department's systems and data.

4.8 Threat Management

Threat Management addresses protection of VDSS systems and data by preparing for and responding to IT security incidents. This component of the Security Program includes Threat Detection, Incident Handling, and IT Security Monitoring and Logging.

4.9 IT Asset Management

IT Asset Management concerns protection of the components that comprise VDSS systems by managing them in a planned, organized, and secure fashion. Asset Management includes IT Asset Control, Software License Management, and Configuration Management and Change Control.

5. COMPLIANCE

All Divisions, Offices, Districts, Regions, and Local Social Service Agencies are responsible for ensuring compliance with IT security policies and standards. The Department measures compliance with IT security policies and standards through processes that include, but are not limited to:

- inspections, reviews, and evaluations;
- monitoring;
- audits; and
- confiscation and removal of IT systems and data.

5.1 Monitoring

5.1.1 General Monitoring Activities

Monitoring is used to improve IT security, to assess appropriate use of Department IT resources, and to protect those resources from attack. Use of Department IT resources

constitutes permission to monitor that use. There should be no expectation of privacy when utilizing VDSS IT resources. VDSS reserves the right to:

a. Review the data contained in or traversing Department IT resources.

b. Review the activities on Department IT resources.

c. Act on information discovered as a result of monitoring and disclose such information to law enforcement and other organizations as deemed appropriate by the CIO.

5.1.2 User Agreement to Monitoring

Any use of Department IT resources constitutes consent to monitoring activities that may be conducted whether or not a warning banner is displayed. Users of Department IT resources:

a. Agree to comply with Department policy concerning the use of IT resources;

b. Acknowledge that their activities may be subject to monitoring;

c. Acknowledge that any detected misuse of Department IT resources may be subject to disciplinary action and legal prosecution.

5.1.3 User Monitoring Notification

Where possible, all IT system users will be notified by the display of an authorized Department warning banner that Department IT systems may be monitored and viewed by authorized personnel, regardless of privacy concerns. This notice shall, at a minimum, appear whenever the IT system user first logs on to the IT system and shall be included in IT security awareness training.

5.1.4 What is Monitored?

Monitoring of VDSS IT systems and data may include, but is not limited to: network traffic; application and data access; keystrokes and user commands; e-mail and Internet usage; and message and data content.

5.1.5 Requesting and Authorizing Monitoring

The CISO or ISO when appropriate has the responsibility to authorize monitoring or scanning activities for network traffic, application and data access, keystrokes, user commands, and e-mail and Internet usage for Department IT systems and data. The CISO and the ISO shall notify each other when appropriate.

5.1.6 Infrastructure Monitoring

Department IT personnel are responsible for maintaining security in their environment through the following processes:

a. Monitoring all systems for security baselines and policy compliance.

b. Notifying the CISO and Department ISO of any detected or suspected incidents.

Note: Installing or using unauthorized monitoring devices is strictly prohibited.

Note: Monitoring the environment infrastructure is a VITA/Northrop Grumman responsibility.

5.2 Internet Privacy

The *Code of Virginia* § 2.2-3803 (B) requires every public body in the COV that has an Internet website to develop an Internet privacy policy and an Internet privacy policy statement that explains the policy to the public and is consistent with the requirements of the *Code*. VDSS' Internet privacy policy and Internet privacy policy statement can be found on the VDSS public web page.

6. Information Security Audits

6.1 Description

The Code of Virginia § 2.2-2009 gives the CIO the responsibility to "*direct the development of policies, procedures and standards for . . . performing security audits of government databases and data communications.*" These policies are outlined in this section; specific requirements are detailed in the *IT Security Audit Standard* (COV ITRM Standard SEC502-00).

6.2 Performance of IT Security Audits

As required by the *IT Security Audit Standard* (COV ITRM Standard SEC502-00), IT Security Audits (audits) shall be conducted by CISO personnel, VDSS Internal Auditors, the Auditor of Public Accounts, or staff of a private firm that, in the judgment of the Department, has the experience and expertise required to perform IT security audits.

Annually, each Department is required to develop and submit to the CISO an audit plan for Department databases. Strictly speaking, a department database is a collection of VDSS data organized into files or tables with accompanying specifications of data objects.

For the purposes of this standard, however, the term "department database" shall include all components of any VDSS IT system in which data resides, and shall also include state Data Communications, as defined below. This definition of "department database" applies irrespective of whether VDSS information is in a physical database structure maintained by VDSS or a third-

party provider. However, this definition does not include databases within VDSS that have been determined by the Department to be non-governmental.

Data Communications includes the equipment and telecommunications facilities that transmit, receive, and validate Department data between and among computer systems, including the hardware, software, interfaces, and protocols required for the reliable movement of information. As used in this section, Data Communications is included in the definition of department database, herein.

The audits conducted under the annual VDSS audit plan must measure compliance with this *Information Technology Security Policy* (COV ITRM Policy SEC500-02) and the *Information Technology Security Standard* (COV ITRM Standard SEC501-01). IT Security Auditors also should also use standards that measure compliance with any other applicable federal and COV regulations.

6.3 Documentation and Reporting of IT Security Audits

After conducting the audit, the auditor shall report the audit results to the Commissioner. The Commissioner shall then require the development of a Corrective Action Plan that includes concurrence or non-concurrence with each finding in the audit report as well as the mitigation strategies. At least once each quarter, the Commissioner or designee shall submit to the CISO a report containing a record of all IT Security Audits conducted by or on behalf of the Department during that quarter. The report must include all findings and specify whether the Department concurs or does not concur with each. The report must also include the status of outstanding corrective actions for all IT Security Audits previously conducted by or on behalf of the Department.

7. Protection of IT Resources

The CISO, in conjunction with the Commissioner through the VDSS ISO or other Administration authorities as necessitated by circumstances, may authorize the confiscation and removal of any IT resource suspected to be the object of inappropriate use or violation of COV IT security laws or policies to preserve evidence that might be utilized in forensic analysis of a security incident.

8. Process for Requesting Exception to IT Security Policy

If the Commissioner determines that compliance with the provisions of the *ITRM Information Technology Security Policy* (COV ITRM Policy SEC500-02) or related standards would result in a significant adverse impact to the Department, the Commissioner may request approval to deviate from that security policy requirement by submitting an exception request to the CISO (see the form attached as the Appendix to this document).

If Division/Office/District/Regional/Local Agency Management determines that compliance with the provisions of VDSS Information Technology Security Polices and Procedures or related standards would result in significant adverse impact to their Division/Office/District/Regional/Local Agency,

the director or senior manager may request approval to deviate from that security policy requirement by submitting an exception request to the VDSS ISO (see the form attached as the Appendix to this document).

Each request shall be in writing and include a statement detailing the reasons for the exception and compensating controls. Requests for exception shall be evaluated and decided upon by the CISO or ISO as appropriate and the requesting party informed of the action taken. Denied exception requests may be appealed to the CIO of the Commonwealth or the CIO of VDSS as appropriate.

9. GLOSSARY

Access: The ability or permission to enter or pass through an area or to view, change, or communicate with an information resource.

Access Controls: A set of procedures performed by hardware, software, and administrators to monitor access, identify users requesting access, record access attempts, and prevent unauthorized access to information resources. Account an established relationship between a user and an information resource.

Access Control: The management of admission to a system and/or to network resources. The first part of access control is authenticating the User, which proves the identity of the User or client machine attempting to log on. The second part is granting the authenticated User access to specific resources based on VDSS policies and the permission level assigned to the User or User Group. (See SEC501-01, Section 13, Paragraph 13.1)

Access Control Administrator: An individual that is appointed in writing by the Data Owner to perform a task on behalf of the Data Owner. This individual may be assigned the task to sign off on computer access forms granting access to the Data Owner databases.

Access Point (AP): A device that connects to a wired network and sends and receives radio signals enabling wireless access to a telecommunication network by wireless devices.

Accountability: The association of each logon ID with one and only one user, so that the user can always be tracked while using an information resource, providing the ability to know which user performed what system activities.

Accreditation: The management approval component of the security certification and accreditation process that constitutes formal acceptance of responsibility for operating the information resource at an acceptable level of risk.

Administrative Security: The management constraints and supplemental controls and procedures established to provide an acceptable level of protection for information resources.

Administrator: The person responsible for applying controls and constraints to provide an acceptable level of protection and for managing user accounts on an information resource. This person is a privileged user.

Advanced Encryption Standard (AES): AES is an encryption algorithm for securing sensitive but unclassified material by U.S. Government agencies.

Agency Head: The director of a department established in the executive branch of state government. (See SEC500- 02, Section 2: Roles & Responsibilities, Paragraph 2.1: Management)

Agency Privacy Officer: See Section 2: Roles & Responsibilities, Paragraph 2.7: Agency Privacy Officer (Where Required by Statute)

Alert: Advanced notification that an emergency or disaster situation may occur.

Alternate Site: A location used to conduct critical business functions in the event that access to the primary facility is denied or the primary facility has been so damaged as to be unusable.

"All personnel": As used in this document, a term that includes Commonwealth employees, contractors, vendors, business partners, and any other authorized users of Commonwealth information systems, applications, telecommunication networks, data, and related resources. It excludes customers whose only access is through public available services, such as public web sites of the Commonwealth. These customers will only be monitored for site security purposes.

Application: A computer program or set of programs that performs the business function for which the information resource is used.

Asset: Any software, data, hardware, administrative, physical, communications, or personnel resource.

Asymmetric Cryptography: A class of cryptographic algorithms that uses separate keys for encryption and decryption.

Attack: An attempt to bypass security controls on an information resource. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the information resource and the effectiveness of existing countermeasures.

Audit: An independent review and examination of records and activities to test for adequacy of controls, ensure compliance with established policies and operational procedures, and recommend changes to controls, policies, or procedures.

Audit Logging: Chronological recording of system activities that is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to its final results.

Authenticate: To determine that something is genuine. To reliably determine the identity of a communicating party or device.

Authentication: The process of verifying the identity of a station, originator, or individual to determine the right to access specific categories of information. Also, a measure designed to protect against fraudulent transmission by verifying the validity of a transmission, message, station, or originator. During the process, the user enters a name or account number (identification) and password (authentication).

Authenticator: The material or credential used to create or implement authentication bindings such as a password, PIN number, token seed, smart card seed, etc.

Authorization: Granting the right of access to a user, program, or process. The privileges granted to an individual by a designated official to access information based upon the individual's job, clearance, and need to know.

Availability: The computer security characteristic that ensures the computer resources will be available to authorized users when they need them. This characteristic addresses backups, alternate sites, disaster recovery, and denial of service.

Backup: The process of producing a reserve copy of software or electronic files as a precaution in case the primary copy is damaged or lost.

Baseline Security Configuration: The minimum set of security controls that must be implemented in all information resources.

Biometric Device: A device that authenticates people by measuring some hard-to-forge physical property, like fingerprints, palm prints, voiceprints, facial scans, or the strokes and timing of a signature.

Biometrics Technologies: used to identify individuals by means of unchanging biological characteristics, such as fingerprints; palm prints; voice prints; or facial, iris, and retina scans.

Buffer Overflow: The presence of more data in a buffer or holding area than the buffer can handle. Often due to a mismatch in processing rates between the producing and consuming processes. This mismatch can result in system crashes or the creation of a back door leading to information resource access.

Business Continuity and Contingency Planning: The process of developing plans and procedures to ensure that the Commonwealth can continue to perform its mission in the event of a business interruption or threat of interruption. (See SEC500-02, Section 15: Business Continuity and Disaster Recovery)

Business Impact Analysis: The process of determining the potential consequences of system unavailability or loss.

Business Partner: A company or individual with whom the Commonwealth has a contractual business relationship.

Campus: Buildings that share telecommunication facilities.

CCMP: (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) is the preferred encryption protocol in the 802.11 i standard.

Certificate Record: signed by an authority holding security information about the user such as a message signed with a public key digital signature stating that a specified public key belongs to someone or something with a specified name.

Certificate Authority (CA): A trusted third-party organization or company that issues digital certificates used to verify the owner of a public key and create public- private key pairs. The role of the CA in this process is to guarantee that the individual granted the unique certificate is who they claim to be. CAs are a critical component in electronic commerce because they guarantee that the two parties exchanging information are really who they claim to be.

Certificate Revocation List (CRL): A list containing names of users and roles that are no longer valid within a public key cryptography system.

Certification: The technical analysis that establishes the extent to which the information resource meets a specified set of security requirements.

Chain of Evidence: Documentation that is sufficient to prove continuous and unbroken possession of a confiscated information resource.

Challenge-Response: An authentication process that sends a challenge to a process that requests authentication. The user or process is authenticated only if the correct response to the authentication request is returned.

Change Control: A management process to provide control and traceability for all changes made to an application system or information resource.

Chief Information Security Officer of the Commonwealth (CIO): The CIO oversees the operation of the Virginia Information Technologies Agency (VITA) and shall, under the direction and control of the Virginia Information Technology Investment Board (the Board), exercise the powers and perform the duties conferred or imposed upon him by law and perform such other duties as may be required by the Board. (See *Code of Virgini*a § 2.2-2005. Creation of Agency; appointment of Chief Information Officer and SEC500-02, Section 2: Roles & Responsibilities, Paragraph 2.4: Chief Information Security Officer of the Commonwealth)

Chief Information Security Officer: (See SEC500-02, Section 2: Roles & Responsibilities, Paragraph 2.5: Director of Security Services)

Cipher Text Message: An encrypted message that cannot be read without encryption keys or technology provided by the sender.

Classified Information (National Security): Information about national defense and foreign relations of the United States that has been determined under Executive Order to require appropriate protection.

Clear Text Message: A message that is sent without encryption. Also known as a plain text message.

Client: A computer system that an end user uses to access services hosted on another computer system called a server. Client may also refer to a program or part of a system that is used by an end user to access services provided by another program (e.g., a web browser is a client that accesses pages provided by a web server).

Commercial-off-the-Shelf (COTS): Software Applications that are sold, leased, and licensed. These applications contain proprietary code that is usually not released to the buyer and is supported and maintained by the vendor, who retains the intellectual property rights.

The Common Criteria (CC): CC addresses protection of information from unauthorized disclosure, modification, or loss of use. The categories of protection relating to these three types of failure of security are commonly called confidentiality, integrity, and availability, respectively. The CC may also be applicable to aspects of IT security outside of these three. The CC concentrates on threats to that information arising from human activities, whether malicious or otherwise, but may be applicable to some non-human threats as well. In addition, the CC may be applied in other areas of IT, but makes no claim of competence outside the strict domain of IT security.

"Commonwealth" or "state": The Commonwealth of Virginia or any of its agencies or departments. (***Code of Virginia*** § 2.2-2200. Definitions)

Compliance Review: A review and examination of records, procedures, and activities to assess the information resource security posture and ensure compliance with established criteria.

Concept of Operations Plan (CONOP): A set of procedures and instructions for using an information resource. Also known as Standard Operating Procedures (SOPs).

Confidentiality: The computer security characteristic that ensures an individual is given access to computer resources based on security clearance and need to know. This characteristic addresses the compromise and inadvertent disclosure of sensitive information. It recognizes that Commonwealth information may be released and shared for legitimate purposes, as long as adequate provisions are taken to protect the data. Confidentiality refers to the controlled conditions in which information is shared or released. These controlled conditions shall be illustrated in additional policies and procedures.

Configuration Management: A formal process for authorizing and tracking all changes to both hardware and software of an information resource during its life cycle.

Contaminated Information Resource: An information resource that could have a detrimental impact on the health or safety of personnel.

Contingency Plan: A set of documented procedures and instructions for responding to emergencies and restoring normal operations following a harmful event.

Continuity of Operations (COOP) Plan: A set of documented procedures developed to ensure the safekeeping of vital resources, facilities, and records; the acquisition of resources necessary for business resumption; and the capability to perform work at alternate work sites until normal operations can be resumed in the event of an emergency or threat of an emergency.

Controlled Area: A restricted work area to which physical access must be limited because of the sensitive or critical function performed or resources located there.

Countermeasure: An action, device, procedure, technique, or other measure that reduces vulnerability or the impact of a threat to an information resource.

Credential: Information passed from one entity to another that is used to establish the sending entity's access rights.

Critical Business Function: A business function necessary for the continued success of the organization. If the business function is non-operational, the organization could suffer serious legal, financial, goodwill, or other serious losses.

Critical Information: Any Commonwealth information that management has designated as essential. The loss or corruption of the information would cause significant financial loss, loss of public trust, hardship, inconvenience, or delay in the mission.

Critical Information Resource: An information resource that performs a process or function that management has designated as essential for correct and uninterrupted Commonwealth operations or essential for the health and safety of Commonwealth personnel.

Cryptography: The protection of information by rendering it unintelligible or unrecognizable until it reaches the intended recipient.

Data: Data consists of a series of facts or statements that may have been collected, stored, processed and/or manipulated but have not been organized or placed into context. When data is organized, it becomes information.

Information can be processed and used to draw generalized conclusions or knowledge. (See SEC501-01, Section 13, Subparagraph 13.1.9: Database, Data Files, and Software Logical Control)

Database: A database is a collection of information organized into interrelated tables of data and specifications of data objects. (See SEC501-01, Section 13, Subparagraph 13.1.9: Database, Data Files, and Software Logical Control)

Data classification: A process of segregating data into sensitive and non-sensitive categories. Its purpose is to provide for protecting information that is sensitive to the Commonwealth. (See SEC501-01, Paragraph 7.3: Data Classification)

Data Dictionary: A collection of descriptions of the data objects or items in a data model for the benefit of programmers and others who need to refer to them. A first step in analyzing a system of objects with which users interact is to identify each object and its relationship to other objects. This process of analyzing a system of objects with which users interact is called data modeling and results in a picture of object relationships. Each object is identified together with its relationship to other objects. (See SEC501-01, Section 14, Subparagraph 14.1.8: Database, Data Files, and Software Logical Control)

Data Owner: The Data Owner is the Department manager responsible for the policy and practice decisions regarding data including case records and documents containing client or confidential information and is responsible for: a) evaluating and classifying the sensitivity of the data; b) defining the protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs; c) communicating data protection requirements to the System Owner; and d) defining requirements for access to the data.

Data Security: Data Security refers to those practices, technologies and/or services used to ensure that security safeguards are applied appropriately to data which is provided, processed, exchanged and/or stored by the Commonwealth. (See SEC501-01, Section 7: Data Security)

Decryption: The process of turning enciphered text back to plain text.

Demilitarized Zone (DMZ): Internet area of increased security that provides protection to Commonwealth information resources that reside outside the Commonwealth intranet.

Determination of Criticality: The process of determining whether and to what degree an information resource is critical.

Determination of Sensitivity: The process of determining whether and to what degree an information resource is sensitive.

Digital Certificate: A password-protected and encrypted file that contains identification information about its holder, a public key, and a unique private key. An individual or server that wishes to send a digitally signed message applies for a digital certificate from a certificate authority (CA). The CA issues an encrypted digital certificate containing the applicant's public key and identification information. The CA makes its own public key readily available. The recipient of an encrypted digital certificate uses the CA's public key to decode the digital certificate attached to the message. The recipient then verifies the certificate as issued by the CA and obtains the sender's public key and identification held within the certificate. With this information, the recipient can verify the owner of a public key.

Digital Signatures: Attachments to an electronic message formed by encrypting a message digest using the private key of a public key encryption pair. A later decryption using the corresponding public key verifies that the signature could only have been generated by the holder of the private key. Digital signatures perform three very important functions: 1. Integrity: A digital signature allows the recipient of a given file or message to detect whether that file or message has been modified. 2. Authentication: A digital signature makes it possible to verify cryptographically the identity of the person who signed a given message. 3. Non-repudiation: A digital signature prevents the sender of a message from later claiming that he or she did not send the message.

Disaster Recovery Plan: A set of documented procedures for extended off-site operations, site clean up, restoration, and disaster recovery should an information resource experience a partial or total loss. Sometimes also referred to as a business resumption plan. (See SEC501-01, Section 15, Paragraph 15.4: Disaster Recovery Plan)

Domain Name Service: A service that translates domain names into IP addresses and vice versa.

Due Care: The customary practice of responsible and sufficient protection of assets that reflects a community or societal norm. Sufficient care of assets should be maintained such that recognized experts in the field would agree that negligence of care is not apparent.

Due Diligence: The level of judgment, care, prudence, determination, and activity that a person would reasonably be expected to provide under a particular circumstance. Due diligence is the prudent management and execution of due care.

Encryption: A means of scrambling data so it cannot be read without the appropriate decryption methodology.

Escrow: Something held in safekeeping.

Evaluation: Investigative and test procedures used in the analysis of security mechanisms to determine their effectiveness and to support or refute specific system weaknesses.

Executive Sponsor: The business manager with oversight of an information resource.

Extranet: A trusted network that connects the Commonwealth to a business partner, who then has access to Commonwealth information resources on the Intranet.

Federal Agency: The United States; the President of the United States; and any department, corporation, agency, or instrumentality heretofore or hereafter created, designated, or established by the United States. (***Code of Virginia*** § 2.2-2200. Definitions)

Firewall: Traffic-controlling gateway that controls access, traffic, and services between two networks or network segments, one trusted and the other untrusted.

Function: A purpose, process, or role.

General Support System: an interconnected set of information resources under the same direct management control which shares common functionality.

Group: A named collection of users created for convenience when stating authorization policy.

Guest Accounts: Logon IDs that allow access to information resources through the use of a generic logon ID that does not utilize a password or utilizes a password known to more than one individual.

Harden: The process of implementing software, hardware, or physical security controls to mitigate risk associated with the Commonwealth infrastructure and/or critical and sensitive information resources.

High Availability: A requirement that the information resource is available 24 hours a day, seven days a week (24x7), or has a low threshold (in seconds or minutes) for down time, or both.

Identification: The process of associating a user with a unique user ID or login ID

IEEE 802.1X: An authentication specification that allows a client to connect to a wireless access point or wired switch but prevents the client from gaining access to the network until it provides credentials, like a user name and password, that are verified by a separate server. In 802.1X, there are three roles: the supplicant (client), authenticator (switch or access point), and authentication server.

Independent Processes: Evaluations conducted by independent personnel, contractors, or vendors for the purpose of applying rigorous evaluation standards to information resources. An independent process is conducted by an organization that is separate and distinct from those responsible for the development and operation of the information resource.

Individual Accountability: The process of associating one and only one user or information resource (such as a workstation or terminal) with any action on an information resource.

Information Assurance: A measure of confidence that the system architecture and features ensure the availability, integrity, authentication, confidentiality, and non-repudiation of the information resource.

Information Custodians: Individuals (often staff within Information Technology) in physical or logical possession of information for Data Owners. (See SE501-01, Subparagraph 7.2.3: Information Custodians)

Information Resources: (1) Encompasses the terms "government information" and 'information technology", as defined in OMB Circular A-130 (FEDSIM, 1993). The data, software, computers, communications networks, and other technology that support the organization. (2) The procedures, equipment, facilities, software and data which are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information. (3) Information resources include data, the processes used to convert this into useful information, the equipment and technology required to use this information and the people involved in making best use of the information.

Information Security: The protection afforded to information in order to preserve the availability, integrity, and confidentiality of the information.

Information Security Officer (ISO): The individual who shall be responsible for the development, implementation, oversight, and maintenance of the Department's information security program. (See SEC500-02, Section 2: Roles & Responsibilities, Paragraph 2.6: Agency Information Security Officer)

Information Technology: means telecommunications, automated data processing, databases, the Internet, management information systems, and related information, equipment, goods, and services. It is in the interest of the Commonwealth that its public institutions of higher education in Virginia be in the forefront of developments in technology. Therefore, the provisions of this chapter shall not be construed to hamper the pursuit of the missions of the institutions in instruction and research. (Source ***Code of Virginia*** § 2.2-2006. Definitions)

Insecure: Unprotected information resource.

Inspection: An official process whereby an information resource is examined carefully and critically.

Instant messaging (sometimes called IM or IMing): A groupware type of communications service that enables an individual to create a private chat room with another individual in order to communicate in real time over the Internet, analogous to a telephone conversation but using text-based, not voice-based, communication. Instant messaging differs from ordinary e-mail in the immediacy of the message exchange and also makes a continued exchange simpler than sending e-mail back and forth.

Integrity: The computer security characteristic that ensures computer resources operate correctly, that data structures are consistent, and that the stored information is accurate (i.e., the data has not been inappropriately altered). This characteristic addresses the deliberate or inadvertent unauthorized manipulation of the information resource and how to maintain the security of the information resource under all conditions.

Integrity Check: Reassures the recipient of a message that the message has not been altered since it was generated by a legitimate source (based on representation of information as numbers and mathematic manipulation of those numbers).

Internet: An external untrusted worldwide public data network using Internet protocols to which the Commonwealth can establish connections. The Commonwealth has no control over the Internet and cannot guarantee the confidentiality, integrity, or availability of its communications.

Intranet: The trusted multi-function (data, voice, video, image, facsimile, etc.) private digital network using Internet protocols, which is operated and maintained for the conduct of Commonwealth business.

Intrusion Detection: A method of monitoring traffic on the network to detect break-ins or break-in attempts either manually or via software expert systems.

ISO/IEC 17799: A code of practice. As such, it offers guidelines and voluntary directions for information security management. It is meant to provide a high level, general description of the areas currently considered important when initiating, implementing or maintaining information security in an organization. The document does not currently cover all areas of importance but is undergoing a thorough revision.

Key: A sequence of data used in cryptography to encrypt or decrypt information. The keys must be known or deduced to forge a digital signature or decrypt an encrypted message.

Key Escrow: The process of storing the encryption key with a third-party trustee to allow the recovery of encrypted text.

Least Privilege: The minimum level of information, functions, and capabilities necessary to perform a user's duties. Application of this principle limits the damage that can result from accident, error, or unauthorized use of an information system.

Local Area Network (LAN): A short distance data communications network used to link computers and peripheral devices (such as printers, CD-ROMs, modems) under some form of standard control. A LAN can be extended with point-to-point wireless access points, thereby extending the coverage area inside large buildings or to nearby buildings within the campus.

Log: To record an action.

Log File: A chronological record of operational and security-related events that have occurred.

Logon ID: An identification code (normally a group of numbers, letters, and special characters) assigned to a particular user that identifies the user to the information resource. (See SEC501-01, Section 6, 6.1.3: Unique User Identification (ID))

Machine Account: Accounts assigned to an information resource or other automated process used to identify actions or requests.

Malicious Code: Harmful code (such as viruses and worms) introduced into a program or file for the purpose of contaminating, damaging, or destroying information resources. Malicious code includes viruses (boot sector, file infector, multipartite, link, stealth, macro, email, etc.), Trojan horses, trap doors, worms, and counterfeit computer instructions (executables). (See SEC501-01, Section 7, Paragraph 7.4: Malicious Code Protection)

Media Access Control (MAC): The hardware address that uniquely identifies each node of a network.

Metropolitan Area Network (MAN): A high speed data intra city network that links multiple locations with a campus, city or LATA.

Mission Critical Facilities: Securing the data center's physical surroundings as well as data processing equipment inside and the systems supporting them to achieve the availability goals of mission critical facilities. (See SEC501-01, Section 10, Subparagraph 10.2.2: Security of Mission Critical Facilities)

Monitoring: Listening, viewing, or recording digital transmissions, electromagnetic radiation, sound, and visual signals.

Network: A series of points or nodes interconnected by communication paths. Networks can interconnect with other networks and contain sub-networks. The term network includes LAN, WAN, MAN, and Campus.

Network Accountability: The process of associating users or information resources with a specific network or logical subnet to a network.

Network Perimeter: A clearly defined boundary established to control the traffic between external untrusted sources and the internal trusted network.

Node: A discrete information resource that is connected to a communications network and participates in the routing of messages within that network.

Nonpublic Available Information Resource: An information resource available only to those users with access to the Commonwealth Intranet, Extranet, or other controlled resources.

Nonrepudiation: A security property that assures the sender cannot deny that he sent the message and the recipient cannot deny that he received it.

Non-sensitive Information: Any Commonwealth information resource that is publicly available. (See SEC501-01, Section 7, Subparagraph 7.3.3: Classification Labels)

Object Reuse: Reassignment and reuse of storage medium that contains one or more objects, after ensuring that no residual data remains on the storage medium.

Official Commonwealth Source: A source approved by authorized Commonwealth management.

Off-site Storage: The process of storing vital records in a facility that is physically remote from the primary site. The facility should be at least 500 yards from the primary site and offer environmental and physical access protection.

One-time Password: A password that can only be used one time.

Operational Workarounds: Manual procedures implemented in the event that the RTO will not be met. These procedures will be sustained until the information resource is restored or the business continuity and contingency plan is implemented.

Out-of-Band Communications: Out of Band, a way to send information (e.g., files) outside the context of normal communications. Out of band communications provide a secondary communications channel for emergencies and/or redundancy. (See SEC501-01, Section 13, Paragraph 13.4: Out-of-Band Communication Alternatives)

Password: A unique string of characters that, in conjunction with a logon ID, authenticates a user's identity.

Penetration Testing: Using teams of specialists to attempt to circumvent the security features of an information resource to identify security weaknesses.

Personnel: All Commonwealth employees, contractors, and subcontractors, both permanent and temporary.

Personal Identification Number (PIN): A short sequence of digits used as a password.

Pilot Project: The initial implementation of a previously untested idea or system that is intended to lend credibility to a project. Also known as a proof of concept project.

Plain Text Message: A message that is sent without encryption.

Pre-Shared Key: A TKIP or CCMP pass-phrase used to protect your network traffic in WPA and WPA2. Some manufacturers use the term "pre-shared secret" instead.

Privacy: The rights and desires of an individual to limit the disclosure of individual privacy information.

Privacy Officer: See Agency Privacy Officer

Private Key: The undisclosed (secret) key in a matched key pair — private key and public key — used in public key cryptographic systems.

Privileged User: A user of an information resource that is able to perform operations not afforded normal users such as system management functions.

Proprietary Information: Material and information relating to or associated with a company's products, business, or activities. This information must have been developed for or by the company and must not be available without restriction from another source.

Public Key: The key in a matched key pair — private key and public key — that is made public (e.g., posted in a public directory) for public key cryptography.

Public Key Cryptography: Cryptography in which the encryption process is publicly available and unprotected but in which a part of the decryption key is protected so that only a party with knowledge of both parts of the decryption process can decrypt the cipher text.

Publicly Available Information Resource: An information resource available through publicly available means, such as the Internet.

Re-accreditation: See accreditation.

Re-certification: See certification.

Recovery: Activities beyond the initial crisis period of an emergency or disaster that are designed to return information resources to normal operating status.

Repudiation: Denial that one did or said something.

Residual Risk: The portion of risk that remains after security measures have been applied.

Restoration: Activities designed to return damaged facilities and equipment to an operational status.

Restricted Data/Information: Information that is restricted based on Commonwealth regulations. (See SEC501-01, Section 7, Subparagraph 7.3.3: Classification Labels)

Revoke: To withdraw, repeal, rescind, cancel, or annul.

Risk: The possibility of loss or injury based on the likelihood that an event will occur and the amount of harm

that could result. (See SEC501-01, Section 2, Paragraph 2.3: Risk Assessment)

Risk Assessment: The process of identifying the vulnerabilities, threats, likelihood of occurrence, potential loss or impact, and theoretical effectiveness of security measures. Results are used to evaluate the level of risk and to develop security requirements and specifications. . (See SEC501-01, Section 2, Subparagraph 2.3: Risk Assessment)

Risk Mitigation: The continuous process of minimizing risk by applying cost-effective security measures commensurate with the relative threats, vulnerabilities, and the value of resources to be protected. (See SEC501-01, Section 2, Paragraph 2.4: Risk Mitigation)

Roles and Responsibility: Roles represent a distinct set of operations and responsibilities required to perform some particular function that an individual may be assigned. Roles may differ from the individual's business title. This document contains the roles and responsibilities associated with implementing information security. The roles and responsibilities are organized as follows***:*** a. High-Level Roles and Responsibilities: Roles and responsibilities for individuals authorized to develop and implement the information security program. Also included are the high-level responsibilities for officers, managers, and all personnel. b. Roles and Responsibilities in Detail: Identifies the roles, detailed responsibilities, and information security activities related to the information security standard described in each section. (See SEC500-02, Section 2: Roles and Responsibilities)

Router: A device or, in some cases, software in a computer, that determines the next network point to which a packet of data should be forwarded toward its destination

Secure: A state that complies with the level of security controls that have been determined to provide adequate protection against adverse contingencies.

Secure Enclave: Intranet area that provides increased security, additional perimeter protection, and access controls for valued information resources.

Secure Shell (SSH): A program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels.

Secure Sockets Layer (SSL): An industry standard protocol for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection.

Security: Security consists of the controls and processes (e.g. policies and procedures, design and implementation of technical measures) established to protect the Commonwealth's sensitive information and systems. Such security measures not only are aimed at protecting privacy, but are aimed at ensuring the authentication, integrity, security, reliability, and availability of information systems.

Security Audit: An independent review and examination of a system's policy, records, and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures. The basic audit objective is to establish accountability for system entities that initiate or participate in security-relevant events and actions. Thus, means are needed to generate and record security audit information and to review and analyze the audit trail to discover and investigate attacks and security compromises. (See SEC501-01, Section 13, Paragraph 13.4: Information Security Auditing)

Security Architecture: The logical and physical security infrastructure made up of products, functions, locations, resources, protocols, formats, operational sequences, administrative and technical security controls, etc., designed to provide the appropriate level of protection for information resources.

Security Breach: The violation of an explicit or implied security policy that compromises the integrity, availability, or confidentiality of an information resource.

Security Controls: The protection mechanisms and controls prescribed to meet the security requirements specified for an information resource. Security controls may include but are not necessarily limited to: hardware and software security features, operating procedures, authorization and accountability procedures, access and distribution controls, management constraints, personnel security, environmental controls, and physical control areas, structures, and devices. Also called security safeguards and countermeasures.

Security Countermeasure: See Security Controls.

Security Features: The security-relevant functions, mechanisms, and characteristics of hardware and software.

Security Incident: An adverse event or situation, whether intentional or accidental, that poses a threat to the integrity, availability, or confidentiality of an information resource. A security incident includes an attempt to violate an explicit or implied security policy.

Security Infrastructure: The facilities, hardware, software, services, protocols, and applications used to transmit, store, process, display, and print information.

Security Mechanisms: See Security Controls.

Security Plan: A strategy for achieving the appropriate level of security controls to be applied. A security plan is designed to identify the appropriate security controls for the information resource and the strategy for their

implementation. The areas to be addressed include hardware, software, connectivity, information, personnel, operating and computing environment, administration, and management.

Security Requirements: The types and levels of protection necessary to adequately secure the information resource.

Security Safeguards: See Security Controls.

Security Service: A service provided by the security infrastructure to help protect an information resource.

Security Specifications: A detailed description of the safeguards required to meet the security requirements and to adequately protect an information resource from unauthorized (accidental or intentional) disclosure, modification, destruction, or denial of service.

Segment: A specially-configured subset of a larger network. The boundaries of a network segment are established by devices capable of regulating the flow of packets into and out of the segment, including routers, switches, hubs, bridges, or multi-homed gateways (but not simple repeaters);

Sensitive Data or Information: Any data or information that has restrictions placed upon its access within the Commonwealth or its disclosure outside of the Commonwealth, as determined by State or Federal Statutes. (See SEC501-01, Section 7, Subparagraph 7.3.3: Classification Labels)

Sensitive Information Resources: Commonwealth information resources that store, process, or transmit sensitive information and/or are susceptible to fraud. (See SEC501-01, Section 7, Subparagraph 7.3.3: Classification Labels)

Separation of Duties: Assignment of responsibilities such that no one individual or function has control of an entire process. Implied in this definition is the concept that no one person should have complete control. Having adequate segregation of duties has a major impact on ensuring that accountability and responsibility for access to information systems is maintained and monitored. (See SEC501-01, Section 11, Paragraph 11.2: Separation of Duties)

Server: An information resource or a set of processes on an information resource providing services to clients across a network.

Service Set Identifier (SSID): A unique identifier attached to the header of packets sent over an IEEE 802.11 wireless network that acts as a password when a mobile device attempts to connect. The SSID differentiates one wireless network from another, so all devices attempting to connect to a specific wireless network must use the same SSID: Other terms for SSID include network name, preferred network, ESSID, and Wireless LAN Service Area.

Shared Accounts: A logon ID or account utilized by more than one entity.

Shared Secret: Information known only to the user and the resource responsible for authentication.

Sign: The process of using a private key to generate a digital signature as a means of proving generation or approval of a message.

Signature: A quantity associated with a message that only someone with knowledge of a user's private key could have generated but which can be verified through knowledge of the user's public key.

Simple Network Management Protocol (SNMP): A standard for gathering data about network traffic and the behavior of network components.

Site Accountability: The process of associating users or information resources with a specific location.

Smart Cards: A tangible object, usually the size of a plastic credit card, which contains a built-in microprocessor that stores and processes information.

Standard of Due Care: The customary practice of responsible and sufficient protection of assets that reflects a community or societal norm. Sufficient care of assets should be maintained such that recognized experts in the field would agree that negligence of care is not apparent.

Standard of Due Diligence: The level of judgment, care, prudence, determination, and activity that a person would reasonably be expected to provide under a particular circumstance. Due diligence is the prudent management and execution of due care.

State: See ***"Commonwealth" or "state***"

Strong Authentication: Authentication normally consisting of two-factor or multi-factor authentication tools, such as a smart card and PIN, or thumbprint and password that support non-repudiation and conclusive tracing of an action to an individual. See ***Authentication***.

Threat: Any circumstance or event (human, physical, or environmental) with the potential to cause harm to an information resource in the form of destruction, disclosure, adverse modification of data, and/or denial of service by exploiting vulnerability.

Time-out: A feature that automatically disables an application, disconnects an information resource, or locks a keyboard after a specified period of idleness.

TKIP: WPA's encryption method is the Temporal Key Integrity Protocol (TKIP). TKIP addresses the weaknesses of WEP by including a per-packet mixing function, a message integrity check, an extended initialization vector, and a re-keying mechanism.

Token: A small tangible object that contains a built-in microprocessor utilized to store and process information for authentication.

Training Accounts: Variants of individual or shared accounts established on a specific information resource for classroom training purposes.

Trusted: Recognized automatically as reliable, truthful, and accurate, without continual validation or testing.

Untrusted: Characterized by absence of trusted status. Assumed to be unreliable, untruthful, and inaccurate unless proven otherwise.

User: An entity that attempts to access an information resource. The entity may be an individual, a computer, or another application.

User ID: A unique symbol or character string that is used by an information resource to identify a specific user. See Logon ID. (See SEC501-01, Section 6, 6.1.3: Unique User Identification (ID))

Version Control: A management process to provide control and traceability of updates to operating systems and supporting software.

Virtual LAN: a network of computers that behave as if they ***are*** connected to the same wire even though they may actually be physically located on different segments of a LAN.

Virtual Private Network (VPN): A private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.

Virus: See Malicious Code.

Vital Record: A document, regardless of media, which, if damaged or destroyed, would disrupt business operations and information flows and result in considerable inconvenience and expense in order to recreate the record.

Vulnerability: A condition or weakness in security procedures, technical controls, or operational processes that exposes the system to loss or harm.

Web Browser: An application that enables users to communicate remotely using Internet protocols with special server-based applications.

Web Server: A server program that provides access to web pages.

Wide Area Network (WAN): A data telecommunications network typically extending a LAN outside a building, over common carrier lines, to link to other LANs that are geographically dispersed. In some situations, point-to-point wireless access points can be used to replace the common carrier lines.

Wired Equivalent Privacy (WEP): A security protocol for wireless networks defined in the IEEE 802.11 standard. WEP provides security by encrypting data over the radio waves as it is transmitted from one end point to another in a wireless LAN, i.e., from access point to laptop. (See SEC501-01, Section 5, Paragraph 5.2: Wireless Security)

Wi-Fi Protected Access (WPA): A vendor consortium agreement based on an early draft of 802.11 i for secure wireless LAN implementation. The agreement covers using TKIP to enhance wireless encryption and security by implementing message integrity checks, better initialization vectors and dynamic keys. WPA also provides for 802.1 X authentication. (See SEC501-01, Section 5, Paragraph 5.2: Wireless Security)

Wi-Fi Protected Access version 2 (WPA2) (IEEE 802.11i Robust Network Security) IEEE standard for secure wireless LAN implementation: The standard is a collection of security features, like IEEE 802.1 X, not a single solution in itself. (See SEC501-01, Section 5, Paragraph 5.2: Wireless Security)

Wireless devices: Any devices, including laptops, notebook personal computers with wireless network interface cards or desktops, that can connect to the state's wired network utilizing 802.11 a, b or g technologies. (See SEC501-01, Section 5, Paragraph 5.2: Wireless Security)

Wireless LAN Gateway: An intermediary device designed to provide segmentation of the wireless LAN from the wired LAN. Such devices include routers, firewalls, and network switches capable of providing VLAN segmentation. (See SEC501-01, Section 5, Paragraph 5.2: Wireless Security)

Workstation: A terminal, computer, or other discrete resource that allows personnel to access and use information resources.

APPENDIX A – IT SECURITY POLICY AND STANDARD EXCEPTION REQUEST FORM (for state agencies)

Any Agency requesting an exception to any requirement of this policy and the related Standards must submit the form on the following page.

IT Security Policy & Standard Exception Request Form

Date of Request: _____

Requester: _____ Agency Name: _____

IT Security Policy or Standard to which an exception is requested:
_____

In each case, the Agency requesting the exception must

1. Provide the **Business or Technical Justification** for not implementing the Standard**:**

2. Describe the scope and extent of the exception:

3. Identify the safeguards to be implemented to mitigate risks associated with the exception:

4. Define the specific duration of the exception (not to exceed six (6) months):

Approved _____ _____
Agency Head Date

Chief Information Security Officer of the Commonwealth (CISO) Use Only

Approved_____ Denied_____ Comments:

_____ _____
CISO Date

Agency Request for Appeal Use Only

Approved_____ Comments:

_____ _____
Agency Head Date

Chief Information Officer of the Commonwealth (CIO) Office Use Only (Appeal)

Appeal Approved_____ Appeal Denied_____ Comments:

_____ _____
CIO Date

APPENDIX B – IT SECURITY POLICY AND STANDARD EXCEPTION REQUEST FORM (for VDSS use)

Any Division/Office/District/Regional/Local Social Service Agency requesting an exception to any requirement of this policy and the related Standards must submit the form on the following page.

IT Security Policy & Standard Exception Request Form

Date of Request: _____

Requester: _____ Division/Office/District/Regional/Local Social Service Agency**: _____**

IT Security Policy or Standard to which an exception is requested:
_____

In each case, the Division/Office/District/Regional/Local Social Service Agency requesting the exception must

1. Provide the **Business or Technical Justification** for not implementing the Standard**:**

2. Describe the scope and extent of the exception:

3. Identify the safeguards to be implemented to mitigate risks associated with the exception:

4. Define the specific duration of the exception (not to exceed six (6) months):

Approved _____ _____
Agency Head Date

Information Security Officer of the Commonwealth (ISO) Use Only

Approved_____ Denied_____ Comments:

_____ _____
ISO Date

Division/Office/District/Regional/Local Social Service Agency **Request for Appeal Use Only**

Approved_____ Comments:

_____ _____
Division/Office/District/Regional/Local Social Service Agency Director Date

VDSS Chief Information Officer (CIO) Office Use Only (Appeal)

Appeal Approved_____ Appeal Denied_____ Comments:

_____ _____
CIO Date